

Master-IT: Project work WS2010/2011

Topic: Evaluation of Vulnerability Testing Tools

Area: Network Security

Start: October 2010
Partner: AIF Project "VuTAT - Vulnerability Tests of AT Components"
Tools: OpenVAS, Nessus, Metasploit-Framework
Prerequisites: Basic knowledge about network protocols and programming.

Motivation

Ethernet based industrial automation networks are often exposed to the same security threats as conventional IT networks. Vulnerabilities of components attached to an automation network might be exploited by an attacker using vulnerability exploitation tools or by disseminating malware (viruses, worms). An actual incident, which gains high attention, is the spread of the so called Stuxnet worm, which has been reportedly crafted to attack a specific control system installation with the intention to sabotage an Iranian nuclear power plant.

The aim of the VuTAT project is to develop a framework that allows the automated test of components for the presence of vulnerabilities.

Goal

Evaluation and comparison of different available tools for vulnerability assessments. In particular it should be analyzed, how these tools could be used to perform a series of automated vulnerability test cases, considering options

- to define new test cases (plugins) using a tool specific scripting languages or the C programming language and
- to integrate test cases form such a tool in some other environment.

Contact: Prof. Dr. Stefan Heiss stefan.heiss@hs-owl.de (Supervisor)
Dipl.-Ing. Andreas Schmelter andreas.schmelter@hs-owl.de